Install & Build Document
Wireless Access Point

For State of Utah WAN Customers
Participating in the State Interoperable Wireless LAN System

Version 1.1
Revised 2/25/04

Document Information

This document was created for the purpose of defining and describing configuration of Wireless Access Points for use on the State of Utah Interoperable Wireless LAN system.

Document Revision

Date of Change	Changes	Change(s) Made	Reason for Change
11/16/03	First Draft		Submitted for Operations Acceptance Teat (OAT)
1/12/04	Second Draft	Team edits.	Resubmission OAT.
2/20/04	Release Draft	Team edits and corrections.	Released for content.
2/25/04	Release Version	Edits for format.	Release version 1.1.

Scope of Document

This document is an instruction manual for the configuration of the State Interoperable Wireless LAN system.

Using this manual, a build engineer should be able to configure a Wireless Access Point to connect to the common access state interoperable 802.11b Wireless LAN environment—from the ground up.

Where possible, step-by-step instructions are provided. However, it is assumed that the audience for this document is well-versed in the following:

Networking Hardware
- Routers
- Switches

Networking Protocols
- RADIUS
- LDAP

Document Contents

The following sections comprise this document:

Overall Architecture
Configuration Overview
Configuring Access Points for RADIUS Services
Configuration of Cisco 1230 Wireless Access Point using IOS

Requirements

Please refer to the Standards and Architecture Document for State Interoperability: 802.11b Wireless environment with port level security (IEEE 802.1x), Version 1.2, January 29, 2004. This document was developed by the ITS 802.11 Wireless LAN product team to describe the technical architecture underlying the state interoperable 802.11 Wireless LAN system and to list the components, by model, that comply with and have been tested to work as part of the system.

As specified in the Standards and Architecture document, Wireless Access Point standards were selected with the following requirements in mind:

802.1x compliant and PEAP authentication capable.
Extensible Authentication Protocol—validating against the Utah Master Directory (UMD).
Enterprise-class deployment, availability and supportability.
Optional: Multiple Wireless LANs—designated by SSIDs (Service Set Identifiers) associated with 802.1q VLAN tagging.

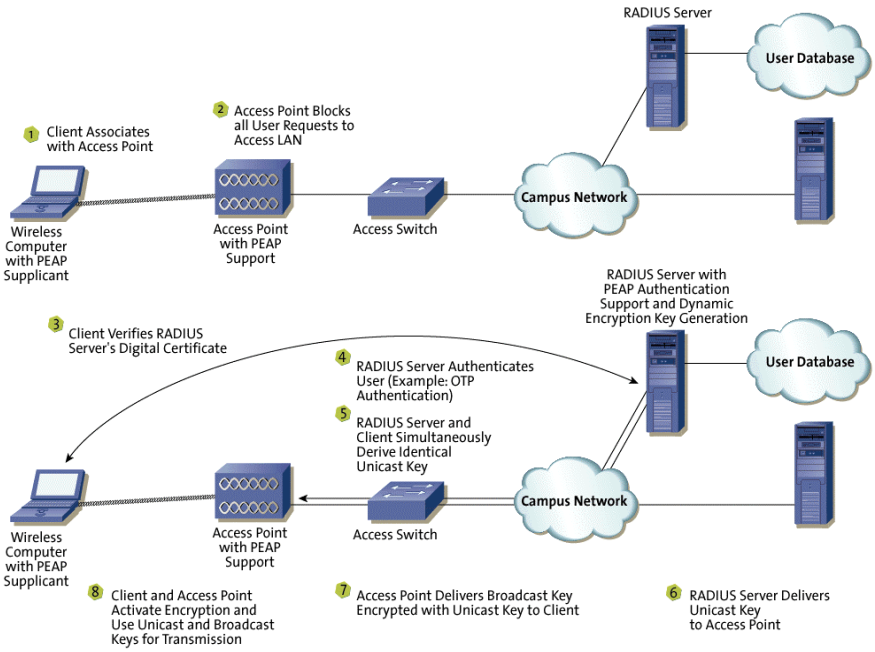
Overall Architecture

The Division of Information Technology Services 802.11 Wireless LAN product is designed for enterprise-class deployment and uses authenticated, authorized access. The Wireless LAN product is based on elements of the WPA (Wi-Fi Protected Access) standard offered by the Wi-Fi Alliance[1] and includes implementation of port-based authentication pursuant to IEEE[2] standard 802.1x and the proposed standards for Extensible Authentication Protocol (EAP) currently before the IETF[3].

The ITS product provides for RADIUS authentication services using the Cisco ACS for Protected EAP authentication in combination with Funk Odyssey client software as the PEAP supplicant for security purposes[4].

Using EAP for authentication and access control protects the Wireless LAN, as the access points will not permit a connection until the user authenticates. This implementation also protects user credentials over a SSL tunnel. Moreover, this approach prevents man-in-the-middle attacks by using dynamic WEP keys derived from unique session information.

High level architecture diagram:



[1] The WiFi Alliance is a group of wireless solution vendors and manufacturers working together to ensure the interoperability of IEEE 802.11*n* wireless Ethernet products—see www.weca.net.
[2] The Institute of Electrical and Electronics Engineers—see www.ieee.org.
[3] The Internet Engineering Task Force—see www.ietf.org.
[4] Additional PEAP supplicants—or client software were tested in the development of this standard. These include AEGIS, by Meetinghouse and ACU, by Cisco Systems. However, the Funk software was selected due to ease of configurability and excellent performance.

The Standards and Architecture Document for State Interoperability: 802.11b Wireless environment with port level security (IEEE 802.1x), Version 1.2, January 29, 2004 lists the specific components—e.g., manufacturer and models—of access points, RADIUS server, 802.11 client and EAP supplicant.

Configuration Overview

Wireless Ethernet security and installation is deceptively simple. Yet this technology relies on the proper functioning of radio transmission and reception—not a skill every LAN Administrator possesses.

Placement of antennae, tuning of radios, installation of wireless access points and the installation and management of clients must be planned and executed properly. In addition, as access point installation involves modifying building facilities, Division of Facilities Construction and Management (DFCM) requirements and potentially other landlord/tenant covenants must be considered. Accordingly, professional installation of Wireless Access Points and antennae are recommended.

Most if not all enterprise-grade wireless access points currently on the market include a Graphical User Interface (GUI) and a Command Line Interface (CLI) for maintenance and support. For many, the device may be accessed directly from the Web Browser

As ITS adds additional Wireless Access Points to the product standard, configuration instructions will be added to this document.

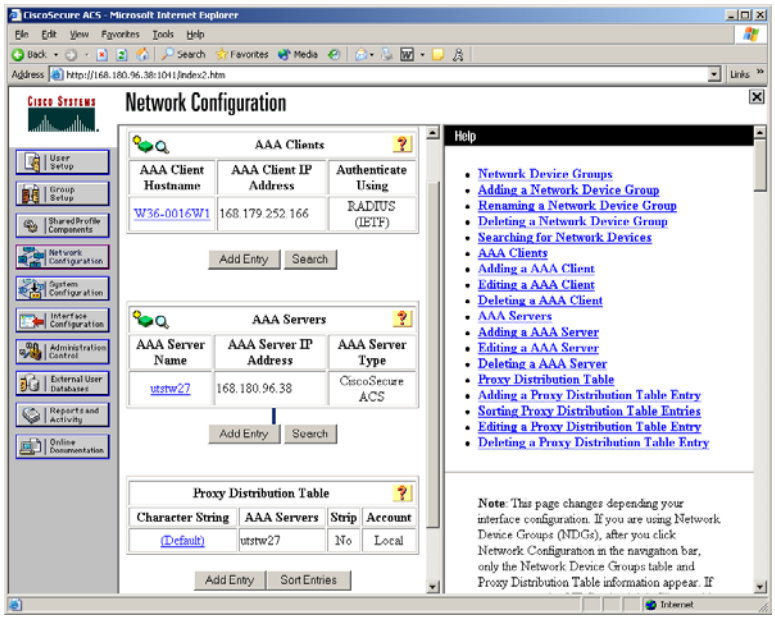
Currently there is one wireless access point model included in the ITS product standard: Cisco Aironet 1230. This access point has both GUI and CLI. While using the GUI can be simpler, it can be more time consuming. Both methods are explained in this document.

Configuring Access Points for RADIUS Services

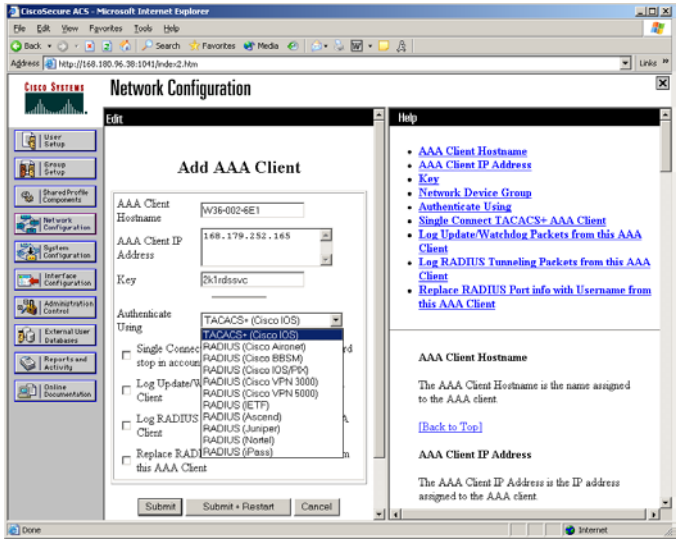
The common element for interoperability of access points and authenticated connectivity is the ability to provide PEAP (Protected Extensible Authentication Protocol) access to the Wireless LAN system.

To configure an access point for the State of Utah interoperable Wireless LAN PEAP, proceed with the following steps:

1. Click on the "Network Devices" button. This displays the configured RADIUS Clients (NAS Servers) ACS Servers and Proxies:



2. To add a NAS (Network Access Server, or RADIUS Client) device, click on the "Add Entry" button. This will bring up the AAA Client Window:

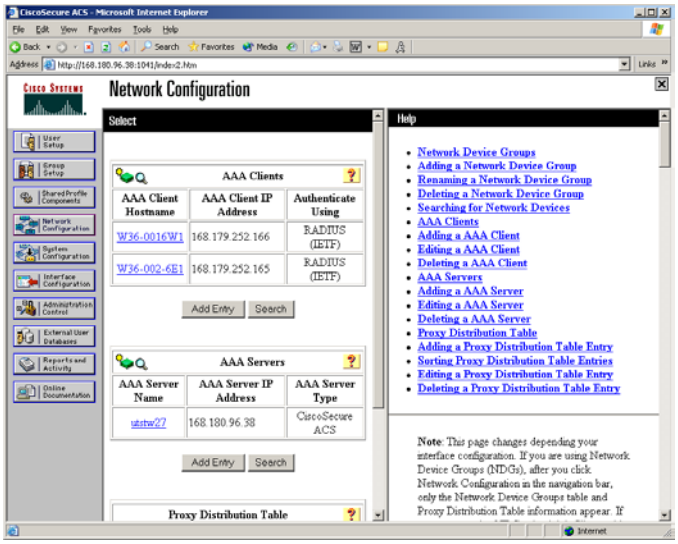


The device's hostname, IP Address and the shared key (default values required by the RADIUS Standard) are displayed. The vendor-specific attributes (VSAs) of the device can be selected from the pull-down menu to specify the authentication method.

Where there are no defined VSAs, it is best to select RADIUS (IETF). This is also selected for Model 1230 Access Points using 802.1x authentication.

The desired logging parameters are then selected. Access points will be submitted as IETF RADIUS clients. Accordingly the "Log Update/Watchdog packets from this AAA Client" and the "Log RADIUS Tunneling Packets from this AAA Client" options will be selected.

3. To save the settings, click on the "Submit+Restart" button. The configured device is then added:



Configuration of Cisco 1230 Wireless Access Point using IOS

Cisco IOS

The standard Cisco paradigm is to store the operating system in flash memory, and the configuration parameters in non-volatile RAM (NVRAM) so the configuration is loaded with the operating system into RAM upon boot.

One of the benefits of devices that run on IOS is that they can be quickly configured using a Telnet session. A standard configuration can be modified with the unique elements of a specific site and within minutes the device is ready for production. This will be the initial approach to installing Wireless Access Points during the first phase of implementation.

The installer will configure the IP Address, subnet mask and default gateway of the Wireless Access Point using a serial cable (included in the Cisco access point package). Then the system will be connected to the network and the rest of the configuration will be added via Telnet.

Standard configurations for both a multiple SSID installation and a single SSID installation are included in this document. The commands described in this document define all the configuration parameters and explain their use.

It is not expected that the installer will configure the device line-by-line. Rather, the needed parameters will be gathered and the standard command files will be modified with the unique settings of each device and each device will be configured via Telnet or SSH. Where possible, the commands, options and settings are described and explained.

Configuration Parameters

Before beginning, ensure that the following information is readily available:

1. A system name for the access point.
   Follow the standard in use at your shop for naming networked devices.

2. The case-sensitive Wireless Service Set Identifier(s) (SSID) for your radio network. **UWDN** is the SSID for the authenticated state interoperable Wireless LAN.

3. A unique IP address for your access, including the default gateway address and subnet mask. **These must be coordinated with your agency's ITS WAN Planner**.
   In order to provide multiple SSIDs (optional—if it meets your agency's needs), the Ethernet interface of the Wireless Access Point must plug into a switch port configured as an 802.1q trunk port.
   If the Wireless Access Point is plugged into a trunk port (for providing multiple SSIDs/VLANs) the IP address of the access point should come from the **native** VLAN of the switch—i.e., the VLAN that does not have .1q tagging on the Ethernet frames.

4. The VLAN ID(s) to be associated with the SSID(s).

5. Unique channel, if there will be multiple Wireless Access Points in this area.

   802.11b has three discrete channels. If there are multiple Wireless Access Points, the channels must be planned and assigned.

   ITS Wireless Services may be consulted to assist with this.

6. SNMP strings, to integrate with your existing devices and process.

Steps to follow

1. Gather and document the parameters identified above.

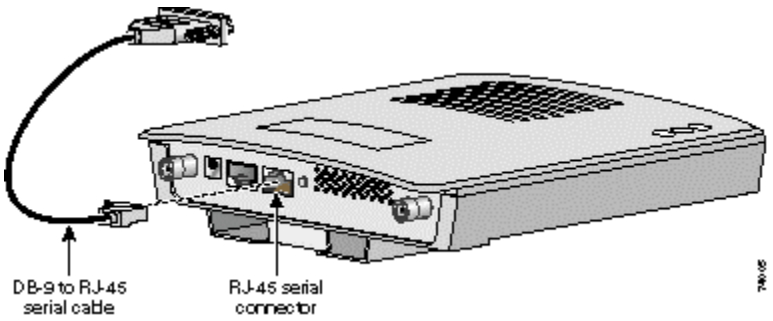
2. Submit the Wireless Access Point name(s) and IP Address(es) to your agency's ITS WAN Planner for entry into DNS (Domain Name Services) and RADIUS services.

3. Modify the text file (either single or multiple SSID). Make sure you change the following parameters:
   a. Host name.
   b. Warning banner—pursuant to your agency standards.
   c. Enter the VLAN IDs—using the text file search for @ and replace them with the values to use. Follow the comments—e.g., an exclamation point (!) signifies the beginning of a comment line. They will need to correspond to the following:
      i. SSIDs
      ii. Radio sub-interfaces
      iii. Ethernet sub-interfaces
      iv. Bridge groups

4. Save the file for remote configuration.

5. Configure the IP Address and default gateway.

   Connect to the Wireless Access Point by the console port. Then enter the IOS configuration mode using Hyperterm or another terminal emulation package. Remember: 9600 baud, 8 data bits, no parity, 1 stop bit and no flow control.



6. Enter the Wireless Access Point's *Privileged Exec* mode by entering the `enable` command and password (the default is Cisco). Configure the enable secret and the BVI1 IP address:

```
ap>
ap> en [password]
ap#
```

The default password must be the first parameter changed. Use the `enable secret` command, since it uses an improved encryption algorithm:

```
ap#configure terminal
ap(config)#enable secret password
```

The access privilege level is also set at this point. The range is from 0-15 where 1 is normal user exec mode and 15 is privileged exec mode. The default is 15. The next step, while optional, will be used for security purposes:

```
ap(config)#service password-encryption
```

This prevents the password from being readable from the configuration file.

7. While still in the *Global Configuration* mode, set the Wireless Access Point IP Address. Rather than assigning IP Addresses to both the radio interface(s) and the Ethernet interface, an IP Address is assigned to the bridge virtual interface—BVI1[5].

```
ap(config)#
ap(config)#interface BVI1
ap(config-int)#ip address 168.179.252.165
255.255.255.192
ap(config-int)#exit
ap(config)#ip default-gateway 168.179.252.129
ap(config)#^z
ap #write memory
```

[5] The bridge-group virtual interface is a normal routed interface that does not support bridging, but does represent its corresponding bridge group to the routed interface. It has all the network layer attributes (such as a network layer address and filters) that apply to the corresponding bridge group. The interface number assigned to this virtual interface corresponds to the bridge group that this virtual interface represents. This number is the link between the virtual interface and the bridge group. When you enable routing for a given protocol on the bridge-group virtual interface, packets coming from a routed interface, but destined for a host in a bridged domain, are routed to the bridge-group virtual interface and are forwarded to the corresponding bridged interface. All traffic routed to the bridge-group virtual interface is forwarded to the corresponding bridge group as bridged traffic. All routable traffic received on a bridged interface is routed to other routed interfaces as if it is coming directly from the bridge-group virtual interface.

8. At this point the Wireless Access Point can be configured via a Telnet session. As noted above, the planned method of deployment is to prepare the configuration file (see explanatory comments in the following section) for each Wireless Access Point to be installed.

   Configure the IP Address and password per the steps above. Then Telnet to the device, copy the new configuration file and paste it to the access point. While using the GUI—the graphical user interface is a method for configuration, it will not be the primary method for systems deployed by ITS. Refer to the section on the browser in the AP 1230 configuration manual.

9. Once the Wireless Access Point has been installed in the appropriate location and connected to the target switch, Telnet to the Wireless Access Point and configure it using the prepared text file.

Sample configuration

```
!---Modify this variable pursuant to your agency naming
standard.
hostname X##-##-#X#

!---Modify this meet your agency legal/security
requirements.
banner motd #
**************************Attention************************
You are accessing a device on the State of Utah Network
If you have reached this machine in ERROR,LOG OFF NOW!

All session activity is logged. Logs will be archived and
may be sequestered for litigation.

Unauthorized access is prohibited and will be prosecuted
to the full extent of the law.
**************************Attention************************
#

!---RADIUS authentication parameters:
aaa new-model
aaa group server radius rad_eap
server 168.179.248.20 auth-port 1812 acct-port 1813
server 172.16.3.16 auth-port 1812 acct-port 1813
aaa group server radius rad_mac
aaa group server radius rad_acct
server 168.179.248.20 auth-port 1812 acct-port 1813
server 172.16.3.16 auth-port 1812 acct-port 1813
aaa group server radius rad_admin
aaa group server tacacs+ tac_admin
aaa group server radius rad_pmip
aaa authentication login default local
aaa authentication login eap_methods group rad_eap
```

```
aaa authentication login mac_methods local
aaa authorization exec default local
aaa authorization ipmobile default group rad_pmip
aaa accounting network acct_methods start-stop group
rad_acct
aaa session-id common

!---Set local administrator access:
username its privilege 15 password 7 07237918621C17061F
username seceng privilege 15 password 7 07092E5E4B070A0C1401
clock timezone T -7
clock summer-time T recurring
ip subnet-zero
dot11 holdoff-time 600
bridge irb
interface Dot11Radio0
no ip address
no ip route-cache

!---Set encryption parameters and keys:
encryption vlan ##n key 1 size 128bit 7
8FAC978DBFCBE2323146564FA7BF transmit-key
encryption vlan ##n mode wep mandatory
encryption vlan ## key 1 size 128bit 7
B1C860B549DD939ED04D2EE2D7C1 transmit-key

!---Configure the SSIDs:
ssid Native
vlan #
authentication shared
ssid St8ofUtahEAPNet
vlan ##
authentication open eap eap_methods
authentication network-eap eap_methods
accounting acct_methods
ssid St8ofUtahWAN
vlan ##n
authentication open
wpa-psk ascii 7
045A09050B244A4F0B1A0112145B5D56797F717E646D7B12051507
speed basic-1.0 basic-2.0 basic-5.5 basic-11.0
rts threshold 2312
channel ####
station-role root

!---This provides compatibility with multiple client cards.
no dot11 extension aironet

!---Cisco Discover Protocol (cdp) is disabled on all radios
!---and Ethernet subinterfaces when VLANs are configured.
no cdp enable
```

```
interface Dot11Radio0.#
encapsulation dot1Q # native

!---Routing parameter to enable route fast switching (CEF)
!---no effect on a sub-interface.
no ip route-cache

!---See above—for better performance cdp is disabled when !-
--using VLANs.
no cdp enable

!---The bridge group parameter “connects” the wireless
!---interface to the wired interface see discussion
!---of bridge groups in the command explanation section.
!---Regardless of the VLAN ID, bridge-group 1 will be
!---associated with the Native VLAN.  These parameters will
!---be configured automatically once the Native VLAN is
!---specified.
bridge-group 1
bridge-group 1 subscriber-loop-control
bridge-group 1 port-protected
bridge-group 1 block-unknown-source
no bridge-group 1 source-learning
no bridge-group 1 unicast-flooding
bridge-group 1 spanning-disabled

!---The sub-interfaces will have the same numeric value
!---as their associated VLAN.  That same numeric value
!---will carry over the bridge groups and the Ethernet
!---and radio sub-interfaces.
interface Dot11Radio0.##
encapsulation dot1Q ##
no ip route-cache
bridge-group ##
bridge-group ## subscriber-loop-control
bridge-group ## port-protected
bridge-group ## block-unknown-source
no bridge-group ## source-learning
no bridge-group ## unicast-flooding
bridge-group ## spanning-disabled
interface Dot11Radio0.##n
encapsulation dot1Q ##n
no ip route-cache
bridge-group ##n
bridge-group ##n block-unknown-source
bridge-group ## port-protected
no bridge-group ##n source-learning
no bridge-group ##n unicast-flooding
bridge-group ##n spanning-disabled
interface FastEthernet0
no ip address
```

```
no ip route-cache

!---Ensure that the speed and duplex values are consistent
!---with the target switch port.
speed 100
full-duplex
ntp broadcast client
interface FastEthernet0.#
encapsulation dot1Q # native
no ip route-cache
bridge-group #
no bridge-group # source-learning
bridge-group # spanning-disabled
interface FastEthernet0.##
encapsulation dot1Q ##
no ip route-cache
bridge-group ##
no bridge-group ## source-learning
bridge-group ## spanning-disabled
interface FastEthernet0.##n
encapsulation dot1Q ##n
no ip route-cache
bridge-group ##n
no bridge-group ##n source-learning
bridge-group ##n spanning-disabled

!---The IP Address and default gateway parameters will
!---have already been configured—this may be removed.
interface BVI1
ip address ###.###.###.### 255.255.255.###

!---Routing parameter to enable route fast switching (CEF)
!---not enable on switches or bridges.
no ip route-cache

!---See above.  The IP Address and default gateway
!---parameters will have already been configured—this may !-
--be removed.
ip default-gateway ###.###.###.X
ip http authentication aaa
ip radius source-interface BVI1
radius-server host 168.179.248.20 auth-port 1812 acct-port
1813 key 7 0873471F1B1D16040408
radius-server host 172.16.3.16 auth-port 1812 acct-port 1813
key 7 00561857165F18151922
radius-server retransmit 3
radius-server attribute 32 include-in-access-req format %h
radius-server authorization permit missing Service-Type
radius-server vsa send accounting
bridge 1 route ip
line vty 5 15
```

```
ntp clock-period 2860622
ntp server 168.180.96.5

!---Remove the default SSID—IMPORTANT security step!!
int dot11radio0
no ssid tsunami
end
copy running-config startup-config
```

System Commands and Settings

Using the hostname command:

```
ap(config)# hostname W36-001-6E1
W36-001-6E1(config)#^z
W36-001-6E1#write memory
```

Banner command:

For legal purposes, ensure that the system banner will be configured with a warning:

```
W36-001-6E1# configure terminal
W36-001-6E1(config)# banner motd #
```

(the # is the delimiter value that ends the text)

```
**************************Attention************************
You are accessing a device on the State of Utah Network
If you have reached this machine in ERROR,LOG OFF NOW!

All session activity is logged. Logs will be archived and
may be sequestered for litigation.

Unauthorized access is prohibited and will be prosecuted
to the full extent of the law.
**************************Attention************************
#
```

This message will be displayed for anyone accessing the Wireless Access Point via Telnet.

Configure administrative access:

The ultimate goal for administering all WAN devices is to authenticate all access to the command line with RADIUS. However, this is not currently in practice, so login ids, passwords and privilege levels should be configured to provide user-specific access to the Wireless Access Point command line.

The IOS command, `username,` creates a user id and (optionally) sets access privilege level. The modifier, `password,` sets the password for the user and the number 7 indicates that the password will be hidden in the configuration file.

```
W36-001-6E1# configure terminal
W36-001-6E1 (config)#username its privilege 15 password 7
L84Lunch
```

Configure time parameters:

The Internetworking Operating System (IOS) allows the administrator to set the system clock, set daylight savings time parameters and assign a NTP (network time protocol) source.

There is also an option to configure an authentication key for communicating with a restricted access time server. Basic NTP server configuration requires the administrator to enter the global configuration mode and specify the NTP server or server group (see above section for optional commands).

```
W36-001-6E1> en [password]
W36-001-6E1#
W36-001-6E1# configure terminal
W36-001-6E1 (config)#ntp server 168.180.96.5
W36-001-6E1 (config)#^z
W36-001-6E1#copy running-config startup-config
```

Remember to save the configuration with either the `write memory` or the

`copy running-configuration startup-configuration` commands.

Configure RADIUS authentication:

The access points will be using RADIUS authentication, first for EAP user authentication, later for administrative access.

Accordingly, the Wireless Access Point needs to be configured to use RADIUS authentication (see above section for the syntax, parameters, and options of the IOS commands).

```
W36-001-6E1# configure terminal
W36-001-6E1 (config)# aaa new-model (this enables AAA—access,
   authorization, and accounting)
W36-001-6E1(config)#aaa new-model
W36-001-6E1(config)#radius-server host 172.16.3.16 auth-
   port 1812 acct-port 1813
W36-001-6E1(config)#radius-server host 168.179.248.20 auth-
   port 1812 acct-port 1813
```

Two RADIUS servers are currently in production. There will soon be four RADIUS servers in production.

Configuring server groups:

Access points can be configured to use server groups for authentication. When configuring these, a subset of servers may be used for a specified service. In configuring the Wireless Access Points per the standard use this command to group the access servers for EAP authentication.

```
W36-001-6E1(config)#aaa group server radius rad_eap
W36-001-6E1(config-sg-radius)#server 172.16.3.16 auth-port
   1812 acct-port 1813
W36-001-6E1(config-sg-radius)#server 168.179.248.20 auth-
   port 1812 acct-port 1813
```

After creating the RADIUS group, enter the servers to be included in this group. Repeat this step for each RADIUS server in the AAA server group. Each server in the group must be previously defined with the **`radius-server host`** command.

Interface configuration:

Administrators should configure the 802.11b (11Mbps) radio first.

Cisco defines the 11b—2.4GHz radio as interface Dot11Radio0, and the 54Mbps, 11a—5GHz radio as the Dot11Radio1 interface. The first version standardizes on 11Mbps 11b and add the additional capabilities of 802.11g and 802.11g as demand and funding exist.

Initial configuration will leave the data rate at the default speed. Trained radio technicians should perform the fine-tuning of radio settings. The initial configuration includes setting the channel or frequency in MHz—megahertz on which the radio

operates. This will avoid interference with other devices[6] and disable the proprietary Aironet extensions to provide compatibility with clients from other manufacturers.

Commands and sequence:

```
W36-001-6E1# configure terminal
W36-001-6E1 (config)# interface Dot11Radio0
W36-001-6E1 (config-if)# channel 2412
W36-001-6E1 (config-if)# no dot11 extension aironet
```

Configuring the SSID (Service Set Identifier):

The SSID is a unique identifier that wireless devices use to initiate and maintain a connection.

SSIDs are case-sensitive and may contain up to 32 alphanumeric characters (no spaces).

Once fully deployed, SSIDs unique to various State services and departments will be available throughout the WAN. Most of the enterprise-class access points on the market today are configurable for multiple SSIDs as long as the wired port is connected to a trunk port on an Ethernet switch with 802.1q trunking enabled.

The Cisco 1230 is currently capable of sixteen separate SSIDs. One SSID must be assigned to the switch's native VLAN, or the VLAN that does not have tagged packets. The management interface of the Access Point (interface BVI1—bridge virtual interface) must be assigned an IP address in the native VLAN.

```
W36-001-6E1#configure terminal
W36-001-6E1(config)# interface Dot11Radio0
W36-001-6E1(config-if)# ssid Native
W36-001-6E1(config-if-ssid)# vlan 1 authentication shared
```

This is the only SSID that is authenticated by a shared key because it will not be assigned an IP network and will be used for access points and bridges only. If an SSID is assigned to a VLAN that relies on a pre-shared encryption key, the authentication is configured as open authentication method and then encryption is required on the VLAN. The following states the method recommended by Cisco:

> "During shared key authentication, the access point sends an unencrypted challenge text string to any device attempting to communicate with the access point. The device requesting authentication encrypts the challenge text and sends it back to the access point. If the challenge text is encrypted correctly, the access point allows the requesting device to authenticate. Both the unencrypted challenge and the encrypted challenge can be monitored, however, which leaves the access point open to attack from an intruder who calculates the WEP key by comparing the unencrypted and

[6] The non-overlapping channels available for use in America are 1, 6, and, 11. The radio can be configured to use any of these bye setting the appropriate frequency—1 = 2412MHz, 6 = 2437MHz, and 11= 2462MHz.

encrypted text strings. Because of this weakness, shared key authentication can be less secure than open authentication[7]."

Be sure to save the configuration frequently with either the `write mem` (**`write memory`**) or the `copy run start` (**`copy running-config startup-config`**) commands.

Steps for configuring multiple VLANs and multiple SSIDs:

Configure on the RadioDot11*N* interface (0—802.11b or g; or 1—802.11a):
- The SSIDs
- The encryption parameters—assigned to the respective VLANs

The Sub-Interfaces—assigned to the VLANs
- The encapsulation (dot1q or other) method

On the SSID interface, configure:
- The associated VLAN
- The authentication method

The generalized syntax includes the following commands:

```
W36-001-6E1#configure terminal
W36-001-6E1(config)#interface dot11radio0
W36-001-6E1(config-if)# ssid ssid-string
W36-001-6E1(config-if-ssid)# vlan vlan-id authentication
   authentication mode   for most SSID's this will be network-eap
W36-001-6E1(config)#interface dot11radio0.1 configure the sub-
   interface on the Wireless Access Point related to the 802.1q native VLAN.
W36-001-6E1(config-if)#encapsulation dot1q vlan-id–in the case of
   the native VLAN, 1 native
W36-001-6E1(config-if)#exit
W36-001-6E1#end
```

The steps require that both:
1. The administrator name the SSID; and,
2. The SSID is assigned to a VLAN—enable the native VLAN on the radio and Ethernet ports as the *native VLAN.*

During the initial phase of deployment only three other SSIDs will be configured in addition to the Native VLAN. These will include the EAP-enabled, authenticated access VLAN, the Shared Key VLAN—for backwards compatibility as administrators migrate users to the authenticated VLAN(s), and, an open, guest VLAN directed to an Internet caching service that will require authentication but no client configuration.

```
W36-001-6E1(config)#interface dot11radio0.##
```

[7] **Cisco Aironet 1100 Series Access Point Installation and Configuration Guide**, **Chapter 10, page 2.**

```
W36-001-6E1(config-if)#encapsulation dot1q ##
W36-001-6E1(config-if)#exit
W36-001-6E1#end
```

Configuring additional SSIDs:

```
W36-001-6E1# configure terminal
W36-001-6E1 (config)# interface Dot11Radio0
W36-001-6E1 (config-if)# ssid St8ofUtahEAPNet
W36-001-6E1 (config-if-ssid)# vlan 23
W36-001-6E1 (config-if-ssid)# authentication open eap
   eap_methods
W36-001-6E1 (config-if-ssid)# authentication network-eap
   eap_methods
W36-001-6E1#configure terminal
W36-001-6E1(config)# interface Dot11Radio0
W36-001-6E1(config-if)# ssid St8ofUtahGBNet
W36-001-6E1(config-if-ssid)#vlan 29
W36-001-6E1(config-if-ssid)#authentication open
W36-001-6E1#configure terminal
W36-001-6E1(config)# interface Dot11Radio0
W36-001-6E1(config-if)# ssid St8ofUtahPSKNet
W36-001-6E1(config-if-ssid)#vlan 100
W36-001-6E1(config-if-ssid)#authentication open
```

Configuring additional VLANs:

```
W36-001-6E1#conf t
W36-001-6E1(config)#int Dot11Radio0
W36-001-6E1 (config-if)#ssid St8ofUtahPSKNet
W36-001-6E1 (config-if-ssid)#encryption vlan 100 key 1 size
   128bit 7 8FAC978DBFCBE2323146564FA7BF transmit-key
   encryption vlan 100 mode wep mandatory
W36-001-6E1(config)#int Dot11Radio0
W36-001-6E1(config-if)# ssid St8ofUtahEAPNet
W36-001-6E1 (config-if-ssid)#encryption vlan 23 key 1 size
   128bit 7 D212FCEDA2E8C707D476F91194EB transmit-key
W36-001-6E1(config-if-ssid)#encryption vlan 23 mode wep
   mandatory
W36-001-6E1(config-if-ssid)#
```

Configuring bridge group parameters

Cisco IOS after version 11.2 integrated routing and bridging—where a specific protocol is both routed and bridged using the bridge group virtual interface (BVI).

As noted above, the bridge-group virtual interface (BVI) is a standard routed interface that does not support bridging, but does represent a corresponding bridge group to the routed interface

The bridge-group "connects" the wired VLAN to the wireless SSID. Some of the settings are automatically added when certain settings are enabled. For example, when a native VLAN is identified (this is the native, non tagged VLAN on the switch port the Wireless Access Point plugs into) the settings for bridge-group are automatically added to this sub-interface and associated to the BVI1 interface. This will be bridge group 1, regardless of the VLAN ID that is actually associated to the native VLAN.

All other bridge groups have the same ID as the VLAN to which they associate, as in the example below (emphasis added):

```
interface Dot11Radio0.23
   encapsulation dot1Q 23
   no ip route-cache
   bridge-group 23
   bridge-group 23 subscriber-loop-control
   bridge-group 23 port-protected
   bridge-group 23 block-unknown-source
   no bridge-group 23 source-learning
   no bridge-group 23 unicast-flooding
   bridge-group 23 spanning-disabled
```

The WLAN sub-interface is associated to the Ethernet sub-interface, and then to the SSID:

```
interface FastEthernet0.23
    encapsulation dot1Q 23
    no ip route-cache
    bridge-group 23
    no bridge-group 23 source-learning
    bridge-group 23 spanning-disabled

ssid St8ofUtahEAPNet
     vlan 23
     authentication open eap eap_methods
     authentication network-eap eap_methods
     accounting acct_methods

interface FastEthernet0.1
    encapsulation dot1Q 1 native
    no ip route-cache
    bridge-group 1
    no bridge-group 1 source-learning
    bridge-group 1 spanning-disabled
```

As noted above, bridge group 1 will be associated to the native VLAN, regardless of the VLAN ID of the native VLAN.

Don't forget to remove the default SSID:

```
(config)# interface dot11radio0
```

```
(config-if)# no ssid tsunami
```